BY ORDER OF THE COMMANDER
AIR FORCE MATERIEL COMMAND (AFMC)

AIR FORCE INSTRUCTION 33-119

AIR FORCE MATERIEL COMMAND
Supplement 1

6 OCTOBER 2000

Communications and Information

ELECTRONIC MAIL (E-MAIL) MANAGEMENT AND USE

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the HQ AFMC WWW site at: https:// afmc-mil.wpafb.af.mil\pdl\.

OPR: HQ AFMC/SCD (Wanda A. Craft) Certified by: HQ AFMC/SC (Venita L. Rhoads)
Pages: 11
Distribution: F

This supplement expands on the guidance in the basic instruction by providing AFMC-specific guidance and policy interpretation. It also implements *AFPD 33-1, Command, Control, Communications, and Computer (C4) Systems.* It applies in part to all Air Force personnel activities, excluding the Air National Guard (ANG) and the United States Air Force Reserve. It also applies to all contractor personnel who manage Air Force programs and the records associated with them, using electronic mail as a means of *official* communications.

AFI 33-119, 1 Mar 99, is supplemented as follows:

1. Use of e-mail to conduct official business takes the place of paper-based communications. Do not print information to paper or mail as hard copy to recipients if e-mail can reach all intended recipients. E-mail takes the place of hard copy communications. It is illegal to modify official e-mail received, as it constitutes an official record transaction. Civil and criminal penalties can be imposed for willful disregard of protection of agency records, which includes e-mail and other kinds of records, regardless of media.

2.2.2. AFMC policy is to use e-mail, as well as the World Wide Web, as a business tool to conduct official business. Functional managers should standardize how e-mail can facilitate work in progress.

2.3. MAJCOM OPR is HQ AFMC/SC. The Information Management (IM) functional OPR is responsible for writing policy and procedures on how to use automation, i.e., a records management application (RMA) software, to manage electronic records. Many e-mails are record in nature; however, until RMA tools are available, follow this supplement to manage e-mail as records.

2.3.2. MAJCOM policies described within this supplement are, in some cases, more restrictive. In AFMC, if a Work Group Manager (WGM) position exists, this same individual serves as the Functional Area Records Manager (FARM). The WGM/FARM oversees the management of ***all*** organizational records, regardless of media. The WGM/FARM should interface with the Centralized Network Control Center (CNCC), end users, and the base records manager to ensure e-mail is properly managed as records.

2.6.1. Commanders' policies should encourage use of e-mail as a way to formally conduct business and move away from the practice to staff work using paper methods. Commanders will develop, publish, and train all employees on local policies. Make sure local policies do not contradict AFI 33-119 or this supplement.

2.6.3. Commanders ensure there is a category in the base clearance paperwork for all employees to verify with the FARM, supervisor, WGM/FARM, or e-mail administrator that ***all*** official records have been properly transferred from desktop, user ID accounts, diskettes, etc., into an official electronic recordkeeping location. Commanders ensure the appropriate people coordinate on clearance paperwork that this has been accomplished prior to e-mail account cancellation. The WGM/FARMs will sign off on base clearance paperwork, verifying that the departing individual has properly screened their hard drive and network shared drive folders to ensure official electronic records are properly identified and transferred to the appropriate location (see paragraphs 8.3, 8.4.1.2, and 8.4.2.2.1). WGM/FARM signature also ensures no restricted information (i.e., individual information) is left on the hard drive.

2.7. Upon RMA implementation, the RMA administrator will ensure e-mail is managed as official records as part of their overall electronic records duties. Records duties described below pertain to the e-mail administrator/WGM/FARM in the CNCC. End-user records duties are covered in paragraph 8 as supplemented.

2.7.1. Contact the base records manager to receive specialized records management training needed to ensure e-mail is properly managed as official records.

2.7.4.3. (Added) Administrators will verify approval with users of individual e-mail accounts and the organizational e-mail account owner prior to destroying e-mail from the mail server. Individual users must, where possible, delete nonrecord items.

2.7.5. (Added) The CNCC has overall responsibility. The RMA administration will provide records oversight and advice to end-users. Until AFMC installs records management software applications on LANs, WANs, etc., preservation of e-mail, as a record, rests with the end user.

2.7.5.1. (Added) E-mail administrator advises end users when their e-mail storage space nears memory capacity. End users may justify need for greater storage capacity when amount of e-mail is deemed official records and/or on-line access is required.

2.7.5.2. (Added) End user requests additional storage space through WGM/FARM and supervisor to e-mail administrator.

2.7.5.3. (Added) E-mail administrator or end-user ensures official e-mail is maintained in a format which cannot be modified. Such storage capability serves as an electronic staging area (see AFI 37-138, *Records Disposition—Procedures and Responsibilities*).

2.8. E-mail end-users include government, contractor, foreign nationals, volunteers, & all others who are granted an e-mail account on a government e-mail system. All must read this AFI and supplement prior to receiving a password to a government e-mail account. Reading this AFI, and supplement, constitutes baseline knowledge of the laws governing use of government e-mail resources and is considered *initial* training. Annual *refresher* training is also required for contractors and foreign nationals. Training may be included with other computer security and/or security awareness training and education (SATE) (see AFI 33-204, *SATE Program*, and as supplemented, and AFI 33-202, *Computer Security Program*, and as supplemented. If commanders require more detailed initial training, it may be delegated to the communications squadron, using this supplement (see para 2.6.1 in AFI and as supplemented).

2.8.1. Use only organizational e-mail accounts to transmit *official* or *formal* e-mail. If desired, include an individual user account as a 'cc' on the e-mail. (This would serve as a 'heads up' of taskings, suspenses, etc.) For record purposes, all e-mail sent or received via organizational e-mail accounts constitute ***official records***. Use Attachment 7 (added) to decide when e-mail is *official* or *formal*. *Formal* e-mail constitutes official taskings, program-specific information, etc., which apply to performance of *official* and *authorized* official duties. Informal e-mail is considered general to the workforce, not related to the duties of the workforce.

- An example of an organizational or formal e-mail would be notification of a tasking to report to a center or squadron commander, the results of a unit compliance inspection (UCI).
- An example of an informal e-mail would be an announcement of a blood drive on the installation. This may be considered non-record or informational only.

2.8.1.1. (Added) First-line supervisors provide/document refresher training. Suggested format is at Attachment 8 (added). Document initial and annual refresher training in personnel records.

2.8.3. Sent and received information must be maintained as part of the e-mail record itself only when the e-mail constitutes orders, direction, or policy of commanders and two-letter directors at Headquarters level. Such e-mail must be transmitted via organizational accounts. Other e-mail users should retain sent and received information only when it will add value to the e-mail record itself. Generally speaking, this kind of information is needed to support decisions and actions of AFMC, especially when the persons sending or receiving the e-mail are critical to validating such decisions or actions.

2.8.5. Recommended level of approval is first line supervisor. However, base-level approval is required on use contributing to meeting Air Force mission and assigned duties. Commanders may delegate this authority to supervisors. At HQ AFMC, approval level is the division chief. Individual approval for each nonofficial Air Force list server is required.

2.8.8. (Added) Encourage use of home pages to post informal or informational data of interest to customers outside the organization. This will help avoid saturating the network and avoid slowing down traffic on the system. Post internal information on electronic bulletin boards. Don't broadcast information to a wide audience if one of the above methods will serve the same purpose.

3. AFMC organizations must establish and use organizational accounts to transmit and receive official taskings, information, etc., when possible. Use organizational accounts when setting up mail groups in lieu of user ID accounts. This minimizes number of changes necessary to keep groups current. Sole use of the organizational account to conduct government business will simplify and standardize official communications. Information transmitted and received via organizational accounts constitute official records.

3.1.1. E-mail users and systems administrators (to include contractor personnel) must be trained on protection of individual information per the *Privacy Act of 1974*. Base Privacy Act officers conduct such training when SATE training doesn't cover this area. The *Freedom of Information Act* (FOIA) requires agencies to respond to requests from the public for access to or copies of official information. This includes requests for e-mail communications. See DoD R 5400.7-R, Air Force, and AFMC supplements to same for specific guidance on FOIA processing. Contact base FOIA manager for specific advice.

3.1.4. (Added) E-mail saved/stored as an official record must be saved in an *unalterable* file.

3.2. It is AFMC policy to only transmit taskings via organizational e-mail accounts where possible.

3.2.1. Individual e-mail accounts should not be used to transmit official taskings. The same chain of command rules apply using e-mail as they do when staffing hardcopy packages. Taskings are levied on

the appropriate receiver by the supervisor. Taskings received by other than through the chain of command may be referred to the supervisor for confirmation. Working files may become official records at the conclusion of work-in-progress actions. Use of workflow software to route, coordinate, request action, report results, etc., is one method of handling work-in-progress. Maintain accountability of all comments, drafts, etc., until conclusion of work-in-progress. If a final decision, document, action, etc., results from the work-in-progress, ensure all appropriate background materials are treated as official records at that time. Usually the record series description (table and rule) from AFMAN 37-139, *Records Disposition Schedule*, provides information on whether background material must be retained as part of the record set.

3.2.1.1. (Added) Exception to this policy exists if web-based coordination or staffing will suffice. Regardless of what automation is used to coordinate and staff work, ensure the procedures are published and familiarize all personnel. Workflow, which includes the ability to do suspense tracking and document management, should provide the best efficiencies and effectiveness for conducting business.

3.2.1.2. (Added) If using e-mail to obtain coordination on attached electronic documents (memorandum, SSS), recommend procedures be developed to ensure needed revisions are accomplished by the offices suggesting revisions.

3.2.1.3. (Added) If staffed electronically, the office in which the signature is obtained:

- Makes all final corrections.
- Annotates the electronic official file copy with the correct date and adds the "//Signed//" above the signature block.
- Files the electronic record in the designated location on the file server.
- Notifies the original OPR that the package is completed.

3.2.2. E-mail users are responsible for the content of the e-mail they create and send. When possible, send e-mail, which is official in nature, via an organizational e-mail account.

3.2.2.1. When using organizational e-mail accounts, the sender may choose to ensure taskings quickly reach the intended receiver by including them as a "***cc***" addressee.

3.2.3.3. If the system cannot provide a unique identifier, publish procedures in the office instruction which provides standard procedures on how organizational accounts are used to conduct business. Employees (primary/alternate) who are appointed to maintain organizational e-mail accounts must be trained on how to forward it to the proper recipient. For accomplishment of taskings, the person maintaining the organizational account may need to forward all taskings to the appropriate level supervisor. The supervisor would then task the appropriate employee, by forwarding tasking to that account. Each organization must establish written procedures to ensure incoming organizational e-mail is read and acted upon promptly, and outgoing organizational e-mail is released only after approval by the releasing authority. Ensure all staff are trained on use of organizational accounts.

3.3.1. Official use may include communicating with contractors, members of the public, or agencies outside the DoD, depending upon the nature of the position. Be sure to protect the interests of the government when communicating outside the DoD. This means not providing restricted, sensitive, or other protected information outside the agency. Keep in mind that some information within the agency including unclassified should only be shared on a need-to-know basis. Privacy Act-related information is one example.

3.3.3.1. Recommended level of approval is first line supervisor. Base approval on use contributing to meeting Air Force mission and assigned duties. Suggest subscribing to organizational accounts (versus individual accounts), if possible.

3.3.3.4. There are many kinds of unclassified, but restricted, information within AFMC. Examples include: Scientific and Technological Information (STINFO), For Official Use Only (FOUO), PA, and proprietary. When in doubt, seek advice from the appropriate program OPRs.

3.4. (Added) Calendars. When e-mail programs offer calendaring features, use them, as much as possible, for scheduling meetings, workshops, etc., rather than maintaining paper calendars. Encourage shared views and calendaring capabilities to improve confirmation dates and times with multiple participants. Calendars for commanders or higher meet the definition of an *official record* unless designated otherwise. Contact the FARM, WGM/FARM, or base records manager for clarification.

4. Commanders should standardize procedures for electronic coordination of e-mail packages. At a minimum, coordinate e-mail with all appropriate/affected offices prior to release. Existing chain of command policies for coordinating, releasing, and replying to administrative communications apply to e-mail. Ensure outgoing organizational e-mail is released only after approval by the releasing authority.

4.2. Forms or memorandum attached to the e-mail transmittal must have a signature facsimile and a date to signify a final product (not a draft). Refer to AFI 33-360, V2, *Forms Management Program*, for specific guidance. For standard forms, use the electronic signature application in the standard electronic forms package or other authorized forms development package for this purpose. (Refer to AFMAN 33-360 for official form use and to AFMAN 33-326, *Preparing Official Communication,* for memorandums).

6.1. Authentication of Air Force records is described in AFI 33-321, *Authentication of Air Force Records*. Paragraph 1.3 defines electronic authentication. E-mail correspondence requiring specific authentication and sent via organizational account should be created in formal memorandum format (see AFMAN 33-326). Otherwise, attach a formal, authenticated memorandum to transmittal e-mail for processing, or copy the memo into the body of the e-mail. When in doubt, format e-mail similar to a formal memorandum with signature block, title, etc.

8.3.3. (Added) If e-mail is 'broadcast' to multiple addressees to user id accounts, the 'receiver' is getting an information copy. One example of a nonrecord, or information copy, is an announcement of an official director's call. Destroy *informational* e-mail sent or received via user ID accounts as soon as possible. It serves as reference or nonrecord material only. Recipients do not have to store their copy as an official record. Instead, they need to annotate their calendars of the event.

8.3.5. (Added) Use the guide in Attachment 7 (Added) to determine whether a particular e-mail must be retained for record purposes. When in doubt, contact the WGM/FARM/FARM or base records manager.

8.4.1.2. OPRs (information owners) must identify, store, maintain, and dispose of official e-mail by their specific record series (retention). If the LAN doesn't provide DISA-certified COTS software designed to manage electronic files by retention, OPRs must ensure they are properly stored and retrievable for the life (retention) of the records. Note that by printing out an email message on paper for filing purposes may not legally satisfy record laws. The electronic version, containing document macro information, may also be maintained in electronic format if possible. When attaching documents (Word, PowerPoint, etc.) to an e-mail; maintain them with the e-mail if needed for record purposes. Note: Only store one copy of any record. Should multiple e-mails address the same attachment or attachments, store the attachments only once in such a way that they can be cross-referenced to the appropriate e-mail(s). If e-mail transmitted

contains the 'FOR THE COMMANDER' line, include transmission data, name(s) of sender, addressee information, and date/time the message was sent as part of the official file (see AFI 33-321). If e-mail is informational only, yet still determined as an official record, it is optional to save addressee information and date/time message was sent. If required, store copy of e-mail on a network drive which allows multiple view/read access only. Ensure the official electronic record cannot be modified.

8.4.1.4. Use of organizational mailboxes generally satisfies the requirement to identify users. If sending to a privately created group e-mail list and the 'FOR THE COMMANDER' line was used, include the complete list of addressees in the electronic file. It is the commander's option to save these lists for additional or future transmissions. If the e-mail package allows, save *receipt* information of taskings from commander or higher levels. Receipt information may also be maintained when it relates to other e-mail messages.

8.4.1.6. When receiving e-mail determined as an official record from outside organizational control in the individual ID account, the following should be accomplished if possible:

- Request sender to use organizational account for future transmissions.
- Staff e-mail through organizational mail account if action is needed.
- File e-mail received in the appropriate location for storage of official files (see above).

8.4.1.6.1. (Added) The owner of the information (official record) content in e-mails is responsible for proper collection, maintenance, and disposition of it. Information owners are responsible for reviewing e-mail and making recommendations as to restriction from release to the public or other agencies. Recommendations should be made after comparing e-mail content to governing directives and or statutes, which may apply. When in doubt, contact the FARM/WGM/FARM, base records manager, or local legal office.

8.4.1.6.2. (Added) E-mail users must maintain e-mail by its record series (table and rule from AFMAN 37-139). It will become the same as all the official records of the office for all e-mail exceeding 2 years retention regardless of whether it was transmitted or received via organizational e-mail account.

8.4.1.7. (Added) If determining an e-mail is official in nature, e-mail users (or information owners) file or archive e-mail requiring retention of 3 years and up to, but not including, permanent retention on a media designated for storage of official electronic records. Prior records manager approval is required to maintain official electronic records (see AFMAN 37-123, *Management of Records*).

- The e-mail administrator (or e-mail server administrator) will store all e-mail sent and received via organizational accounts for 2 years [See paragraph 3.1.4 (Added)]. The administrator will ensure:
- All stored e-mail is retrievable upon request, with associated attachments.
- All stored e-mail cannot be modified in any way.
- All stored e-mail is identifiable by the author and/or receivers.
- Procedures must be developed to migrate e-mail in conjunction with insertion of new technology to ensure accessibility/readability of e-mail.

8.4.2.2.1. (Added) A recordkeeping system on a network is defined as hardware and software that allows for electronic search and retrieval, storage of the electronic file which automates the disposition instructions for each record series, and which will ensure the electronic file is maintained for its legally-defined timeframe. If this feature is not available, the owner of the information must manually screen the electronic files at least annually to perform disposition actions.

8.4.2.2.2. (Added) Until RMA is in place, owners of the e-mail documents will store all official e-mail on an alternate media; such as c: drive or floppy diskette, according to retention requirements. The WGM/ FARM is a major participant in the development of a standard way to store such material and assists with implementation and oversight.

- As an example, if an office maintains 3-year, 5-year, and 10- year records, establish a separate storage location for each retention.
- In this example, if storing on diskettes, label three separate diskettes with the required information - one for 3-year files; one for 5-year files; and one for 10-year files. This will simplify destruction; information on one disk will have same retention requirements.

8.4.2.2.3. (Added) If the user determines the e-mail sent or received is considered ***record*** in nature, it is his/her sole responsibility to move such e-mail to an authorized recordkeeping storage location or contact the WGM/FARM for assistance.

8.4.2.2.4. (Added) Owners of official record copies of e-mail, sent or received, may store it on either the *c: drive* or a floppy diskette if the RMA is not in place. Make sure the location column of the file plan shows electronic storage information and that the records requirements in this supplement are met. NOTE: Permanent retention records must be retained in hard copy (or paper) in order to satisfy National Archives and Records Administration criteria. Contact the WGM/FARM for assistance if desiring to keep permanent e-mail or other official records in electronic format.

8.4.2.2.5. (Added) Regardless of which drive is used, set up a subdirectory by folders which describe the appropriate record series of the e-mail. Obtain this information from the RIMS-approved file plan for the office.

8.4.2.2.6. (Added) If storing on diskettes, label them using identifying categories similar to the examples listed below:

OFFICIAL FILES

OFFICE SYMBOL

Item number(s) from RIMS file plan, table(s) and rule(s)

CLASSIFICATION/OTHER RESTRICTIONS, i.e., PA, etc.

8.4.2.2.7. (Added) File floppy diskette in the first file folder of the file cabinet for the official records. This folder contains the hard copy of the RIMS file plan. If the office does not have hard copy (paper) records, file the diskette in a location that clearly designates it as containing the official files of the office. Note: Always back-up electronic records stored on diskettes or local hard drives.

8.4.2.2.8. (Added) Screen diskette/drive at least annually to erase or delete those electronic files eligible for destruction.

8.4.2.3. Informal e-mail content (that which is sent or received via user ID accounts) should ***not*** be official, or record, in nature. Instead, it should be deemed as informational or non-record and considered of transitory value to the individual or agency. Storage of not longer than 90 days is recommended.

9.2.1. Internets are considered unsecured. Therefore, consider all e-mail traffic via internet, at a minimum, to be sensitive but unclassified (SBU). Use encryption as required to protect information content.

9.2.3. If suspecting unauthorized use or access to e-mail or other AIS, immediately contact the WGM/ FARM, e-mail administrator, or supervisor.

9.4.2. Do not transmit individual information protected by the Privacy Act (see AFI 33-332, *Air Force Privacy Act Program*) over unsecured e-mail, the World Wide Web, or Internet without encryption. Do not transmit individual information over e-mail or Internet without encryption. If encryption capability is not available, use faxogram, regular mail channels, or express mail to transmit information (see AFI 33-332 for additional information).

9.4.2.1. Never send individual information about an individual, to include name linked with SSAN, to groups of people. The Privacy Act requires only providing individual information to an authorized individual. Generally speaking, this would be a supervisor or authorized personnel office staff member. Contact the base Privacy Act officer or legal office for specific advice.

9.4.2.2. (Added) *Never* create a database or AIS containing two or more individual identifiers without proper approval as a Privacy Act (PA) system of records (see AFI 33-332 and AFMC supplement).

9.4.2.3. (Added) Prior to converting a hard copy PA system of records to electronic media, contact the base PA officer and base records manager for advice.

9.4.3. Mark information exempt under the FOIA as For Official Use only and encrypt prior to transmission over the Internet or e-mail.

9.6.4. (Added) E-mail Security. The CNCC will routinely monitor accounts for possible violations (i.e., receipt of pornography), and report through appropriate channels. Such reporting will apply to senders and receivers. Investigative agencies, i.e., OSI, will be provided individual e-mail account information (audit trails, history) upon receipt.

Attachment 7 (ADDED)
HOW TO DETERMINE AN E-MAIL'S 'OFFICIAL RECORD' STATUS

A7.1. All senders and recipients of e-mail must be able to answer the following. If the answers are all, or mostly, yes, ***you*** are responsible for maintaining ***official records***. If answers result in no, the e-mail is non-record, or informational in value. Always ask the Functional Area Records Manager (FARM) or Work Group Manager (WGM) for assistance if unclear as to the nature of the e-mail. If answers result in an ***official record*** category for the e-mail, the record must be retained for the legal retention of such a record.

QUESTION(S) TO CONSIDER
Did I create the e-mail?
Does the content or attachment to the e-mail directly relate to my program, project, position with the government or in other official capacity?
Did I provide opinions, advice, or mission-specific comments?
Did I obligate the organization or agency in any way?
Does the content of the e-mail reflect the content of other records maintained in the office regardless of media?
Have I been identified or tasked to perform some action?
Am I involved in the content of the e-mail in other ways, such as, meetings, reviews, etc?
Did my supervisory chain transmit the e-mail to me with directions to perform in some way?
Is the subject matter something related to the function or mission of the organization in general or my position/program in particular?
Do I already maintain official records, in any media, on the same subject or content?
Does the material describe agency methods, processes, policies, and decisions or does the material affect the public?

Attachment 8 (ADDED)

SAMPLE E-MAIL TRAINING OVERVIEW

Training Categories	Local Subject Matter Expert/ Phone/e-mail*	References	Material Briefed (X)
SECURITY	E-mail administrator or COMSEC/OPSEC section	AFI 33-202/AFMC Sup 1	
Information Security	"	Specific AFI or AFMC Sup	
Operational Security	"	"	
System Security	"	"	
PROFESSIONAL COURTESIES	E-mail administrator or supervisor	AFI 33-119	
LOCAL OI	Author	OI Number	
USER RESPONSIBILITIES	Self Explanatory	AFI 33-119_AFMC Sup 1	
RECORDS MGT REQUIREMENTS	FARM	AFI 37-123, AFI 138, AFI 139, AFI 33-119_AFMC Sup 1, AFI 33-322	
AUTHORIZED USE	E-mail administrator or supervisor	AFI 33-119	
UNAUTHORIZED USE	"	AFI 33-119	
SYSTEM OPS AND CAPABILITIES	E-mail administrator	AFI 33-series	
PRIVACY ACT REQUIREMENTS	FARM or PA monitor	AFI 33-332 & AFI 33-119	
PUBLIC RELEASE OF INFO/FOIA	FOIA monitor or supervisor	DoDR5400.7, AF & AFMC Sups, AFI 33-119, & AFI 33-129	
OTHER:			

_____ ____ _____

Employee Signature Supervisor Signature

List specific personnel in this column. Entries represent suggested experts.

DEBRA L. HALEY
Director of Communications & Information